GSA®

Cybersecurity Supply Chain Risk Management Guide

GSA
August 2022
Version 2.0

Table of Contents

1. Executive Summary

Commercially available technology solutions offer significant benefits:

- Low cost;
- Interoperability;
- Rapid innovation;
- Product feature variety; and
- The ability to choose from competing vendors.

Commercial products, whether proprietary or open source, can meet the needs of a global base of public and private sector customers. However, the same globalization and other factors that allow for such benefits can also increase the risk of a threat event. That threat can directly or indirectly affect cybersecurity within the supply chain—often undetected—and result in risks to all parties.

Agencies are concerned about the risks associated with products and services that may contain potentially malicious functionality, are counterfeit, or are vulnerable due to poor manufacturing and development practices affecting cybersecurity within the supply chain. These risks are associated with an enterprise's decreased visibility into, and understanding of, how the technology they acquire is developed, integrated, and deployed, as well as the processes, procedures, and practices used to assure the security, resilience, reliability, safety, integrity, availability, and quality of the products.

Cybersecurity supply chain risks may include, but are not limited to, theft of intellectual property, insertion of counterfeits, unauthorized production, tampering, theft of hardware, insertion of malicious software and hardware, data leaks, information system breaches, as well as poor development and manufacturing practices affecting cybersecurity within the supply chain.

This guide is intended to provide agencies with a high-level description of Cybersecurity Supply Chain Risk Management (C-SCRM) and resources for acquiring products and services that align with C-SCRM best practices.

Agencies are at different levels of maturity in securing their cybersecurity supply chains. General Services Administration (GSA) offers agencies cybersecurity resources such as Highly Adaptive Cybersecurity Services (HACS) and Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Approved Products List (APL) Continuous Diagnostics and Mitigation (CDM) Tools on the Multiple Award Schedule (MAS). Beyond commercial products off MAS, many other solutions can be bought and implemented to support C-SCRM critical success factors as described in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161 Rev.1, addressing C-SCRM practices for systems and organizations.

Questions about this guide? Need subject matter expertise on C-SCRM and other IT needs? Use Section 7, Contact Information for this C-SCRM Guide.

2. Audience

C-SCRM is an enterprise wide activity. This publication is intended to serve a diverse audience involved in managing cybersecurity risk in federal organizations, and especially those responsible for C-SCRM activities. This includes individuals with:

- System, information security, privacy, or risk management and oversight responsibilities;
- System development responsibilities;
- Acquisition and procurement-related responsibilities;
- Logistical or disposition-related responsibilities;
- Security and privacy implementation and operations responsibilities; and
- Security and privacy assessment and monitoring responsibilities.

3. What is Cybersecurity Supply Chain Risk Management (C-SCRM)?

NIST defines C-SCRM in SP 800-161 Rev.1 as a systematic process for:

- Managing exposures to cybersecurity risk in the supply chain;
- Guarding against threats, and vulnerabilities throughout the supply chain; and
- Developing risk response strategies to the cybersecurity risk in the supply chain presented by the supplier, the supplied products and services, or the supply chain itself.

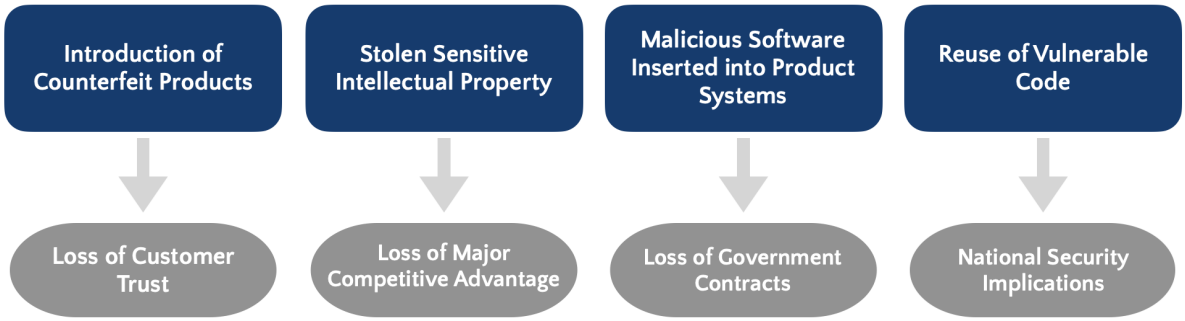
Cybersecurity Risk
Cybersecurity risk in the supply chain is the potential for harm or compromise that arises from the cybersecurity risks posed by suppliers, their supply chains, and their products or services. Employees, vendors, and privileged users can all leak sensitive data and personal information outside the organization.

The most common cybersecurity risks in any given supply chain affecting organizations include:

- Data leaks, such as external and internal attackers;
- Information system breaches which usually occur when a malicious actor infiltrates an operating system or network without permission; and
- Malware attacks that happen through ransomware that encrypts data until the organization pays a ransom.

Examples of cybersecurity risk in the supply chain include, but are not limited to, the following:

Figure 1: NIST's Examples of the Impact Cybersecurity Risks Have on the Supply Chain



- An organized criminal enterprise introduces counterfeit products into the market resulting in a loss of customer trust and confidence;
- Insiders working on behalf of a system integrator steal sensitive intellectual property resulting in loss of a major competitive advantage;
- A proxy working on behalf of a nation-state inserts malicious software into supplier-provided product components used in systems sold to government agencies. A breach results in loss of several government contracts; and
- A system integrator working on behalf of an agency reuses vulnerable code leading to a breach of mission critical data with national security implications.

Cybersecurity risks such as these happen when vulnerabilities are not managed throughout the supply chain.

4. NIST C-SCRM

NIST SP 800-161 Rev.1 provides guidance to organizations on how to identify, assess, and mitigate cybersecurity supply chain risks at all levels. The publication integrates C-SCRM into risk management activities by applying a multi-level, C-SCRM-specific approach, including guidance on developing:

- C-SCRM strategy implementation plans;
- C-SCRM policies;
- C-SCRM plans; and
- C-SCRM risk assessments for products and services.

NIST SP 800-161 Rev.1 also provides examples of C-SCRM control families that include relevant controls and supplemental guidance to help mitigate risk to information systems and components, as well as the supply chain infrastructure.

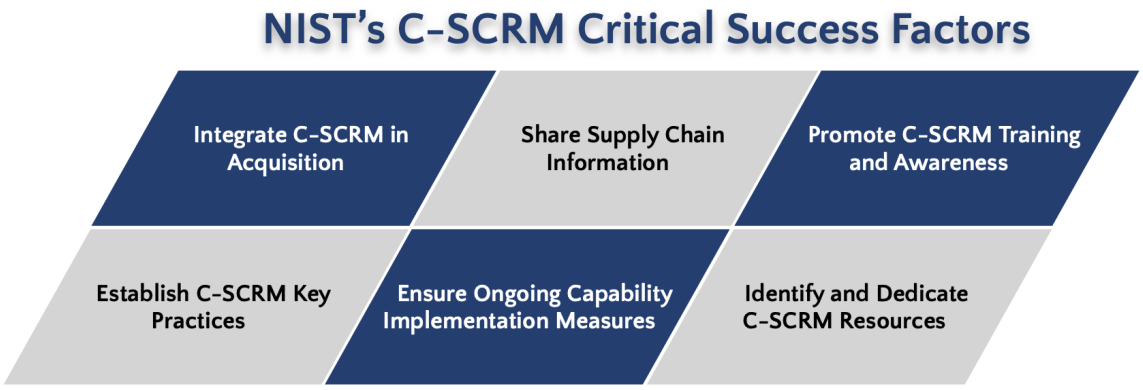
NIST SP 800-161 Rev.1 C-SCRM Critical Success Factors

To successfully address evolving cybersecurity risk in the supply chain, enterprises need to:

- Set up multiple internal processes and capabilities;
- Communicate and collaborate across enterprise levels and mission areas; and
- Ensure all individuals within the enterprise understand their role in managing cybersecurity risk in the supply chain.

NIST has identified six critical factors to C-SCRM success in SP 800-161 Rev.1. These include:

Figure 2: NIST's Critical Factors to C-SCRM Success



1. **Acquisition –** Integrating C-SCRM considerations into acquisition activities is essential to improving management of cybersecurity risk in the supply chain at every step of the procurement and contract management process.

   This life cycle begins when a purchaser identifies a need. It includes the processes to plan for and describe requirements, conduct research to identify and assess viable sources of supply, solicit bids, and evaluate offers to ensure they conform to C-SCRM requirements and assess C-SCRM risk associated with the bidder and the proposed product and/or service offering.

   After contract award, the purchaser must ensure the supplier satisfies the terms and conditions described in their contractual agreement and that the products and services conform as expected and required. C-SCRM considerations must be addressed at every step in this life cycle.

2. **Supply Chain Information Sharing –** Enterprises are continuously exposed to risks that come from their supply chains. An effective information-sharing process helps to ensure enterprises can get information they need to understand and mitigating cybersecurity risk in the supply chain. They can also share information to others who might suffer the same risks.

3. **Training and Awareness –** Many within the enterprise contribute to successful C-SCRM. These may include information security, procurement, risk management, engineering, software development, IT, legal, and human resources (HR). The enterprise should foster an overall culture of security, including C-SCRM as an integral part. The enterprise can use many ways to foster the culture. Traditional awareness and role-based training are only one part.

4. **Key Practices –** C-SCRM builds on existing standard practices in many disciplines, as well as ever-evolving C-SCRM capabilities. NIST outlines these three types of C-SCRM practices:

   - **Foundational -** Your agency must have foundational practices in place to successfully and productively interact with system integrators. Use these practices to improve your enterprise's ability to develop and execute more advanced C-SCRM practices.
     Example: Develop a process for identifying and measuring the criticality of the enterprise's suppliers, products, and services.

   - **Sustaining -** Use sustaining practices to enhance the efficacy of cybersecurity supply chain risk management. These practices include and build upon foundational practices.
     Example: Define, collect, and report C-SCRM metrics.

   - **Enhancing** - Apply enhancing practices to advance toward adaptive and predictive C-SCRM capabilities. Pursue these practices the agency has broadly implemented and standardized sustaining practices across the enterprise.
     Example: Enhance enterprise leadership's ability to identify optimal risk responses with quantitative/probability analysis.

NIST SP 800-161 Rev.1 provides additional examples of C-SCRM foundational, sustaining, and enhancing practices.

5. **Capability Implementation Measurement and C-SCRM Measures –** Enterprises must actively manage their C-SCRM's programs' efficiency and effectiveness through ongoing measuring of the programs themselves. Enterprises can use several methods. All methods rely on a variety of data collection, analysis, contextualization, and reporting activities. Collectively, use these methods to track and report progress and results that show reduced risk exposure and improved enterprise security outcomes.

6. **Dedicated Resources** – To appropriately manage cybersecurity risk in the supply chain, dedicate funds towards this effort. Identifying resource needs and taking steps to secure adequate, recurring, and dedicated funding are essential and important steps that need to be built into the C-SCRM strategy and implementation planning effort and included in an enterprise's budgeting, investment review, and funds management processes.

   Access to adequate resources allows an agency to establish and sustain a C-SCRM program capability. The continued availability of dedicated funds will allow enterprises to sustain, expand, and mature their capabilities over time.

5. Cybersecurity and Infrastructure Security Agency (CISA) Information and Communications Technology (ICT) SCRM Task Force

In December 2018, CISA established the ICT SCRM Task Force with representatives from the public and private sectors. Its goal is to identify challenges and develop workable solutions for managing risks to the global ICT supply chain. The task force provides many resources for organizations to use:

- Fact sheets;
- Infographics;
- Threat scenario reports;
- Vendor SCRM templates;
- Lessons learned; and
- Acquisition guidance documents.

In addition, the ICT SCRM Toolkit includes strategic messaging, social media, videos, and resources. It emphasizes the role all stakeholders have in securing ICT supply chains.

6. C-SCRM Products and Services

Agencies will be at varying levels of maturity when it comes to developing C-SCRM programs and implementing controls to mitigate cybersecurity supply chain risks. GSA provides customer agencies with multiple ways to buy the products and services needed such as:

- Vendor risk management tools, which allow organizations to research and vet vendors;
- Identity, Credential, and Access Management (ICAM) and Mobile Identity Management services, which ensure that only authorized users can access to agency data, systems, and facilities; and
- Other products and services that can be applied to security controls to mitigate supply chain risk.

Agencies benefit from choosing GSA solutions because we offer a commitment to meet customer needs, easy access to the best solutions, cost savings, and compliance with increasingly complex federal regulatory guidance.

GSA also has solutions (See Appendix A below) that fully integrate procurement with C-SCRM processes for the customer, such as 2nd Generation IT (2GIT). This is a tailored replacement program for expiring IT hardware platforms, software solutions, ancillary supplies, and services.

Agencies can get C-SCRM related products and services through the GSA Technology Purchasing Programs listed in Appendix A – *GSA-Offered Products, Services, and Solutions for C-SCRM* that address cybersecurity-specific risk factors and how to start an agency C-SCRM program.

7. Contact Information for this C-SCRM Guide

Use these contacts to ask questions about this guide or find subject matter experts to assist with C-SCRM or other IT needs:

- E-mail ITSecurityCM@gsa.gov for Customer Support with the C-SCRM Guide.
- E-mail CIAP@gsa.gov for any feedback or suggestions to improve the C-SCRM Guide.
- Contact the agency-assigned Customer and Stakeholder Engagement (CASE) National Account Managers (NAMs) for acquisition support for the GSA solution identified in Appendix A of this C-SCRM Guide.

Appendix A – GSA-Offered Products, Services, and Solutions for C-SCRM

The following table lists GSA Technology Purchasing Programs that provide C-SCRM related products, services, and solutions. GSA can provide options to meet your C-SCRM needs.

For additional information, reach out to your agency-assigned National Account Manager (NAM).

Table 1. C-SCRM Guide for GSA-Offered Products, Services, and Solutions

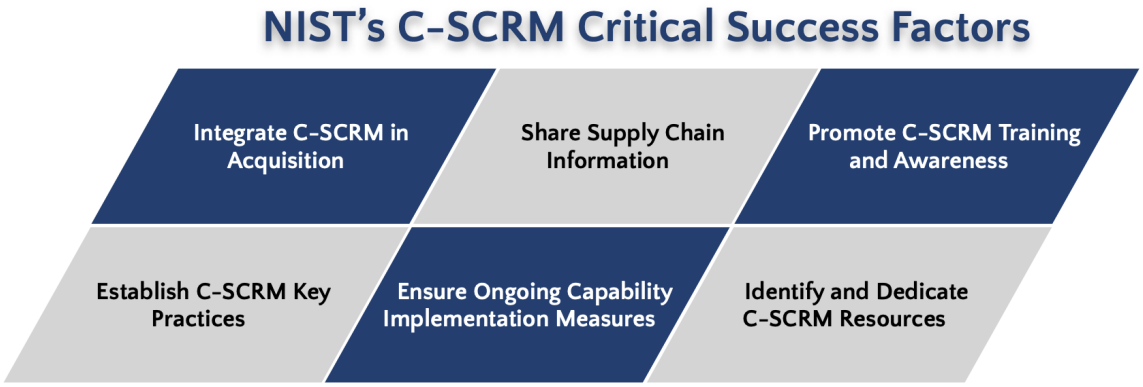
GSA Technology Purchasing Program	Solution	Description
Multiple Award Schedule (MAS)	Highly Adaptive Cybersecurity Services (HACS) SIN 54151HACS	HACS includes a range of services, such as the seven-step Risk Management Framework (RMF) services, information assurance, virus detection, network management, situational awareness and incident response, secure web hosting, and backup, security services, and Security Operations Center (SOC) services. HACS vendors are cataloged under five (5) subcategories: High Value Asset Assessments, Risk and Vulnerability Assessments, Cyber Hunt, Incident Response, and Penetration Testing.
Multiple Award Schedule (MAS)	Identity, Credential, and Access Management (ICAM) Tools SIN 541519ICAM	ICAM Tools SIN includes managed service offerings for electronic credentials (Identity Assurance Level [IAL], Authenticator Assurance Level [AAL], and Federation Assurance Level [FAL] assurance levels), identity and access management, authentication, and identity and access management professional services.
Multiple Award Schedule (MAS)	GSA Advantage CDM APL Tools	CDM Tools includes DHS APL hardware and software. CDM capabilities include: Asset Management, Identity and Access Management, Network Security Management, and Data Protection Management.
Multiple Award Schedule (MAS)	Mobile Identity Management SIN 517312	Wireless Mobility Solutions, include, but are not limited to, the following: Wireless Carrier Services Enterprise Mobility Management (EMM) services include mobility infrastructure, Mobility-as-a-Service (MaaS), Enterprise Mobility Management, Mobile Backend-as-a-Service (MBaaS), and Telecom Expense Management (TEM) Mobile Application Security services include, but are not limited to, Mobile Application Vetting, Mobile Threat Protection (MTP), Mobile Identity Management Internet of Things (IoT) and Other/Mobile Services
Multiple Award Schedule (MAS)	IT Professional Services SIN 54151S	IT Professional Services include, but are not limited to, database planning and design; systems analysis, design, and implementation; programming; conversion and implementation support; network services; data/records management; and testing.
Multiple Award Schedule (MAS)	Data Breach Response & Identity Protection Services SIN 541990IPS	Data Breach Response and Identity Protection Services (IPS) includes an integrated, total solution to provide identity monitoring and notification of Personally Identifiable Information (PII) and Protected Health Information (PHI); identity theft insurance; identity restoration services; and protecting (safeguarding) the confidentiality of PII and PHI.
Multiple Award Schedule (MAS)	Risk Assessment and Mitigation Services SIN 541990RISK	Risk Assessment and Mitigation Services includes: breach mitigation and analysis/forensic services, the deployment of financial risk assessment and mitigation strategies and techniques; improvement of capabilities through the reduction, identification, and mitigation of risks; detailed risk statements, risk explanations and mitigation recommendations; design and development of new business applications, processes, and procedures in response to risk assessments; and ensuring compliance with governance and regulatory requirements. Under this SIN, firms can also assist the Ordering Agency with preventive measures in protecting Personally Identifiable Information (PII) and Protected Health Information (PHI) through the evaluation of threats and vulnerabilities to PII and PHI type of information; training of Government personnel on how to prevent data breaches and identity theft; vulnerability assessments; privacy impact and policy assessments; review and creation of privacy and safeguarding policies; prioritization of threats; maintenance and demonstration of compliance; and evaluation and analysis of internal controls critical to the detection and elimination of weaknesses to the protection of PII and PHI type of information.

Table 1. C-SCRM Guide for GSA-Offered Products, Services, and Solutions		
Governmentwide Acquisition Contracts (GWACs)	Alliant 2	Alliant 2 is a multiple-award, indefinite-delivery, indefinite-quantity (IDIQ) GWAC that will enable federal civilian agencies and the Department of Defense (DOD) to provide Information Technology (IT) services and IT services-based solutions from the most qualified businesses. The basic contract offers comprehensive and flexible IT solutions worldwide including infrastructure and related services, applications and related services, and IT management services to support agencies' integrated IT solution requirements.
Governmentwide Acquisition Contracts (GWACs)	VETS 2	VETS 2 is a multiple award, IDIQ GWAC set aside exclusively for service-disabled veteran-owned small business firms. VETS 2 provides Federal agencies with customized IT services and IT services-based solutions, both commercial and non-commercial, as defined in the Clinger-Cohen Act and FAR 2.101.
Governmentwide Acquisition Contracts (GWACs)	GSA 8(a) STARS III	The Best-in-Class 8(a) STARS III GWAC is a small business set-aside contract that provides flexible access to customized IT solutions from a large, diverse pool of 8(a) industry partners. The 8(a) STARS III GWAC: ● Expands capabilities for emerging technologies, ● Supports both outside of the continental United States (OCONUS) and CONUS requirements, and ● Features limited protestability up to $10M.
Other Programs	Enterprise Infrastructure Solutions (EIS)	EIS is a comprehensive solution-based vehicle to address all aspects of Federal agency IT telecommunications, and infrastructure requirements.
Other Programs	2nd Generation Information Technology Blanket Purchase Agreements (2GIT BPAs)	2GIT incorporates SCRM as a foundational feature to secure the supply chain for customers. By awarding to industry partners with solid enterprise SCRM plans, GSA helps to address the cybersecurity vulnerabilities associated with IT products. 2GIT also offers: ● Access to mission-critical, best-value IT from a diverse pool of more than 70 industry partners including more than 50 small businesses. ● Solutions that meet current procurement policies, incorporate best practices (like collecting prices paid data), and track savings/cost reduction. ● Options that support the Fiscal Year 2019 SECURE Technology Act and other federal cybersecurity efforts.
Other Programs	Federal Risk and Authorization Management Program (FedRAMP)	FedRAMP is a government-wide program that promotes the adoption of secure cloud services across the federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies.

Appendix B – Key Takeaways

Overview of Cybersecurity Risk in the Supply Chain

- Agencies face cybersecurity risk from suppliers, their supply chains, and their products or services.
- The most common cybersecurity risks in any given supply chain affecting organizations include data leaks, information system breaches, and malware attacks.
- Cybersecurity risks happen when vulnerabilities are not managed throughout the supply chain. To successfully address evolving cybersecurity risk in the supply chain, enterprises must implement:



- NIST develops reliable and practical standards, guidelines, tests, and metrics to help manufacturers, retailers, government agencies, and other organizations with their C-SCRM.
- GSA helps improve C-SCRM by establishing GSA-specific considerations related to C-SCRM during various stages of the acquisition, consistent with NIST guidelines.

C-SCRM Products, Services and Resources

GSA gives customer agencies multiple ways to procure the products and services that can be applied to security controls to mitigate supply chain risk. Agencies can use GSA's HACS SIN, DHS CISA CDM APL Tools, and many other solutions to support C-SCRM critical success factors.

Buy these and other C-SCRM related products and services through the GSA Technology Purchasing Programs listed in Appendix A – *GSA-Offered Products, Services, and Solutions for C-SCRM*.

Also, CISA developed an ICT SCRM Toolkit that includes strategic messaging, social media, videos, and resources for all stakeholders to use in securing ICT supply chains.

GSA has subject matter expertise to assist with C-SCRM or other IT needs:

- E-mail ITSecurityCM@gsa.gov for C-SCRM Guide Customer Support.
- E-mail CIAP@gsa.gov for feedback or suggestions to improve this guide.
- Contact the agency-assigned Customer and Stakeholder Engagement (CASE) National Account Manager (NAM) for acquisition support for the GSA solution from Appendix A.